Amendments to the Specification

Please replace Paragraph **[0019]** with the following marked-up replacement paragraph:

-- To achieve the foregoing objects, and in accordance with the purpose of the invention as broadly described herein, the present invention may be provided as methods~~, systems, and/or computer program products. In one aspect, techniques are providing~~ for achieving context-sensitive confidentiality among security domains within a federated environment that spans a plurality of security domains, further comprising: determining a route to be taken by a content request message to be transmitted from a content requester in the federated environment to a content provider in the federated environment[[,]] (wherein: [[where]] the route comprises a network transmission path which begins at the content requester and ends at the content provider and passes through a plurality of intermediary nodes, each of the intermediary nodes located between the content requester and the content provider on the network transmission path; the route is determined by consulting stored policy that specifies, for the content receiver sending the content request message to the content provider, the network transmission path; and the route spans a plurality of the security domains); storing the determined route at a network-accessible location; determining, prior to transmitting the content request message from the content requester, a plurality of portions of the content request message that are security-sensitive, further comprising using a context to consult stored policy that identifies the security-sensitive portions which are applicable to that context, wherein the context comprises an identification of the content requester, an identification of the content provider, and a message type identifying the content request message; determining, prior to transmitting the content request message from the content requester, rights of each of the intermediary nodes~~ to be encountered on the determined

~~route~~ to access each of the determined security-sensitive portions of the content request message, further comprising consulting stored policy for each of the intermediary nodes, wherein the stored policy specifies whether this intermediary node is entitled to access this security-sensitive portion of the content request message; specifying, in unencrypted form in the content request message, the message type, an identifier of the network-accessible location where the determined route is stored, and a plurality of message receiver elements, wherein a separate one of the message receiver elements is specified for each of the intermediary nodes that is entitled to access each of the security-sensitive portions, the separate one specifying an identification of that intermediary node as a permitted receiver of that security-sensitive portion and a node-specific keyword corresponding to that intermediary node; selectively protecting the security-sensitive portions of the content request message, according to the determined access rights by encrypting, for each of the security-sensitive portions of the content request message, that security-sensitive portion separately for each distinct one of the intermediary nodes which is entitled to access that security-sensitive portion and storing that separately-encrypted security-sensitive portion in the content request message in association with the node-specific keyword corresponding to that distinct one of the intermediary nodes, thereby enabling each of the intermediary nodes to locate and access each of the security-sensitive portions which it is entitled to access and preventing that intermediary node from accessing any of the security-sensitive portions which it is not entitled to access; and transmitting the content request message with its selectively-protected portions from the content requester to the content provider on the determined route (wherein: the transmitted content request message contains information identifying an authentication authority from a first of the security domains and an identification of a party for which the content request message

requests access to services and indicates that the identified authentication authority has already authenticated the party using security credentials of the party in the first security domain; the intermediary nodes and the content provider, upon receiving the content request message in other ones of the security domains, can bypass authentication of the party for access to services of that other security domain, upon verifying authenticity of the authentication authority, establishing that the authentication authority vouches for the received content request message, and using the identification of the party to locate previously-stored security credentials for the party which are usable within that other security domain; and the security credentials for the party in at least one of the other security domains are different from the security credentials of the party in the first security domain). --

Please cancel Paragraphs **[0020]** through **[0027]**.